Socio-Economic Problems and the State
journal home page: http://sepd.tntu.edu.ua


ISSN 2223-3822

Sorokivska, O., Kinal, N. & Stefaniv, R. (2026) The investment component of project-oriented information security management for small and medium enterprises on the path to the EU digital market. Socio-Economic Problems and the State (electronic journal), Vol. 34, no. 1, pp. 71-82. URL: http://sepd.tntu.edu.ua/images/stories/pdf/2026/26soaedm.pdf

ІНВЕСТИЦІЙНА СКЛАДОВА ПРОЄКТНО-ОРІЄНТОВАНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ НА ШЛЯХУ ДО ЦИФРОВОГО РИНКУ ЄС

Олена СОРОКІВСЬКА | **Назар КІНАЛЬ** | **Руслан СТЕФАНІВ**

Тернопільський національний технічний університет імені Івана Пулюя
вул. Руська, 56, м. Тернопіль, 46001, Україна

e-mail: sorokivska_o@tntu.edu.ua
ORCID ID: https://orcid.org/0000-0001-8549-2910

e-mail: nazarkinal@ukr.net
ORCID ID: https://orcid.org/0009-0003-7980-2101

e-mail: amrg-pg@ukr.net
ORCID ID: https://orcid.org/0009-0002-2129-3454

Article history:
Received: 24.02.2026
1st Revision: 09.04.2026
Accepted: 17.04.2026

JEL classification:
L86
G32
M15

UDC:
330.341:004.738.5

DOI:
https://doi.org/10.33108/sepd2026.01.071

Анотація. *У статті досліджено інвестиційну складову проєктно-орієнтованого управління інформаційною безпекою малих та середніх підприємств (МСП) в умовах інтеграції до цифрового ринку Європейського Союзу. Обґрунтовано, що вихід українських МСП на Єдиний цифровий ринок ЄС супроводжується подвійним викликом: необхідністю одночасної цифрової трансформації бізнес-процесів і приведення системи управління ризиками у відповідність до вимог європейського регуляторного середовища. Доведено, що інформаційна безпека перестає бути допоміжною IT-функцією та набуває статусу стратегічного чинника конкурентоспроможності й доступу до ринку. У роботі проаналізовано вплив ключових нормативно-правових актів ЄС – зокрема General Data Protection Regulation (GDPR) та NIS2 Directive – на формування вимог до кіберстійкості підприємств, що здійснюють транскордонну діяльність. Показано, що комплаєнс у сфері захисту персональних даних і кібербезпеки виступає не лише регуляторною вимогою, а й економічною умовою участі у цифрових ланцюгах постачання, залучення інвестицій та укладення контрактів із європейськими партнерами. Методологічну основу дослідження становить поєднання інструментарію інвестиційного менеджменту та проєктного підходу до управління інформаційною безпекою. Запропоновано застосування показників очікуваних річних збитків (ALE) та рентабельності інвестицій у безпеку (ROSI) для кількісного обґрунтування доцільності впровадження заходів кіберзахисту в умовах обмежених фінансових ресурсів МСП. Розроблено модифіковану модель чистої вигоди (Net Benefit), що доповнює традиційні розрахунки показником приросту вартості доступу до ринку (Market Access Value, ΔMAV). Такий підхід дозволяє врахувати не лише ефект зниження ризиків і уникнення штрафних санкцій, а й додатковий маржинальний дохід, отриманий завдяки виконанню вимог комплаєнсу. На основі гіпотетичного фінансового сценарію продемонстровано, що навіть за від'ємного значення ROSI у короткостроковій перспективі інвестиції в інформаційну безпеку стають економічно виправданими у середньостроковому періоді, а з урахуванням ΔMAV можуть забезпечувати позитивний фінансовий ефект вже протягом перших років реалізації проєкту. Обґрунтовано, що низький рівень інформаційної безпеки створює регуляторні, фінансові, репутаційні та контрактні бар'єри для виходу українських МСП на цифровий ринок ЄС. У підсумку зроблено висновок, що трансформація підходу до управління інформаційною безпекою – від витратної моделі до інвестиційної – є необхідною умовою забезпечення стійкості, конкурентоспроможності та інтеграції українських МСП до цифрового економічного простору Європейського Союзу. Запропонований підхід може бути використаний як методичний інструментарій для стратегічного планування бюджетів кібербезпеки та обґрунтування інвестиційних рішень у процесі євроінтеграції бізнесу.*

Ключові слова: *інвестиційний менеджмент, інформаційна безпека, МСП, проєктно-орієнтоване управління, цифрова трансформація, ринок ЄС, ROSI.*

Сороківська О., Кіналь Н., Стефанів Р. Інвестиційна складова проєктно-орієнтованого управління інформаційною безпекою малих та середніх підприємств на шляху до цифрового ринку ЄС. Соціально-економічні проблеми і держава. 2026. Вип. 1 (34). С. 71-82. URL: http://sepd.tntu.edu.ua/images/stories/pdf/2026/26soaedm.pdf

1. Постановка проблеми.

В умовах євроінтеграції українські малі та середні підприємства опиняються в ситуації структурного «подвійного тиску». З одного боку, вихід на Єдиний цифровий ринок ЄС вимагає прискореної цифрової трансформації бізнес-процесів: впровадження хмарних сервісів, електронного документообігу, CRM/ERP-систем, онлайн-платежів, інтеграції з європейськими платформами та маркетплейсами. Цифровізація стає не конкурентною перевагою, а базовою умовою доступу до партнерств, ланцюгів постачання та фінансових інструментів ЄС.

З іншого боку, така цифрова експансія автоматично підвищує поверхню атаки та рівень кіберризиків. Вимоги ЄС, зокрема щодо захисту персональних даних, управління інцидентами, безперервності бізнесу та доведеної кіберстійкості, передбачають не формальну наявність технічних засобів, а системне управління ризиками, аудит безпеки, навчання персоналу та документовані процедури реагування. Для українських МСП це означає необхідність інвестувати у кібербезпеку паралельно з інвестиціями у цифрові технології.

Проблема полягає в тому, що фінансові ресурси більшості МСП є обмеженими, а доступ до довгострокового капіталу – ускладненим. У результаті підприємства змушені одночасно модернізувати ІТ-інфраструктуру та забезпечувати її відповідність європейським стандартам безпеки, що створює конфлікт пріоритетів між розвитком і захистом. Недостатнє фінансування кіберстійкості може призвести до інцидентів, які нівелюють переваги цифровізації, тоді як надмірні витрати на безпеку без економічного обґрунтування стримують інноваційний розвиток. Отже, подвійний виклик полягає у необхідності синхронізувати темпи цифрової трансформації з економічно обґрунтованими інвестиціями у кібербезпеку, щоб забезпечити одночасно конкурентоспроможність на ринку ЄС і фінансову стійкість бізнесу.

Емпіричне підтвердження цього подвійного виклику простежується у міжнародній статистиці кіберінцидентів. Аналітичні звіти провідних організацій демонструють, що саме сектор МСП є одним із найбільш уразливих у сучасному цифровому середовищі, а наслідки атак для малого бізнесу мають критичний, а подекуди й екзистенційний характер. Це означає, що питання кіберстійкості для українських підприємств у процесі євроінтеграції є не теоретичним, а безпосередньо пов’язаним із їх виживанням і здатністю працювати на ринку ЄС.

2. Аналіз останніх досліджень та публікацій.

Теоретико-методологічний фундамент дослідження базується на синтезі класичних теорій інвестиційного менеджменту та сучасних підходів до проєктно-орієнтованого управління. Зокрема, використання фундаментальних праць Г. Марковіца [1] та В. Шарпа [2] дозволило адаптувати принципи формування та оптимізації інвестиційного портфеля до специфіки активів інформаційної безпеки. Водночас методологічні розробки К. Керцнера [3] та М. Хамфрі [4] стали основою для розгляду системи захисту інформації не як статичного стану, а як ітераційного процесу проєктних удосконалень, що відповідає динаміці сучасного бізнесу.

Аналіз емпіричних даних провідних міжнародних інституцій підтверджує критичну вразливість сектору малого та середнього підприємництва (МСП) у глобальному кіберпросторі. Згідно з результатами Verizon Data Breach Investigations Report [5], малий бізнес залишається мішенню для майже половини всіх реєстрованих атак, а дані National Cyber Security Alliance [6] свідчать про те, що відсутність інвестицій у безпеку призводить до банкрутства 60% таких компаній протягом пів року після інциденту. Дослідження агентства ENISA (Cybersecurity Threat Landscape for SMEs) [7]

додатково деталізують цей ландшафт, ідентифікуючи фішинг та програми-вимагачі як ключові вектори загроз, що потребують пріоритетного фінансування.

Важливою складовою сучасних наукових розвідок є вивчення нормативно-правового поля Єдиного цифрового ринку ЄС. Аналіз регламенту GDPR (General Data Protection Regulation) [8] та директиви NIS2 (Directive 2022/2555) [9] доводить, що комплаєнс у сфері безпеки перетворюється з технічного питання на стратегічну економічну умову доступу до європейських ринків. Розгляд пакету цифрового регулювання, зокрема Digital Services Act (DSA) [10], Digital Markets Act (DMA) [11] та Data Act [12], дозволяє визначити нові правила відповідальності та умови обміну промисловими даними, які безпосередньо впливають на інвестиційну політику підприємств.

Методичний апарат оцінки ефективності витрат на безпеку в наукових публікаціях останніх років зміщується у сферу кількісного аналізу. Використання показників ALE (очікувані річні збитки) та ROSI (рентабельність інвестицій у безпеку) дає змогу математично обґрунтувати доцільність впровадження захисних заходів в умовах обмежених ресурсів МСП. Крім того, застосування індексів DESI (Digital Economy and Society Index) [13] дозволяє об’єктивно оцінити рівень цифрової інтенсивності суб’єктів господарювання та їхню готовність до інтеграції в цифровий простір Євросоюзу.

3. Постановка завдання.

Мета дослідження полягає в теоретичному обґрунтуванні інвестиційної природи проєктно-орієнтованого управління інформаційною безпекою малих та середніх підприємств та розробці методичного підходу до оцінки економічної ефективності таких інвестицій в умовах інтеграції до Єдиного цифрового ринку Європейського Союзу.

Для досягнення поставленої мети було визначено та вирішено такі завдання:

– проаналізовано вплив ключових нормативно-правових актів ЄС, зокрема Регламенту GDPR та Директиви NIS2, на формування нових вимог до кіберстійкості та комплаєнсу підприємств, що здійснюють транскордонну діяльність;

– обґрунтовано необхідність трансформації підходу до управління інформаційною безпекою – від традиційної витратної моделі до проєктно-орієнтованої інвестиційної моделі, що дозволяє забезпечити гнучкість та масштабованість систем захисту відповідно до потреб бізнесу;

– запропоновано методичний інструментарій для кількісного обґрунтування доцільності впровадження заходів кіберзахисту в умовах обмежених фінансових ресурсів МСП із використанням показників очікуваних річних збитків (ALE) та рентабельності інвестицій у безпеку (ROSI);

– розроблено модифіковану модель оцінки чистої вигоди (Net Benefit), яка, на відміну від традиційних підходів, враховує показник приросту вартості доступу до ринку (ΔMAV) як стратегічний економічний ефект від виконання вимог європейського комплаєнсу;

– на основі розрахунку фінансових сценаріїв продемонстровано економічну виправданість та терміни окупності проєктів із забезпечення інформаційної безпеки, враховуючи як зниження ризиків, так і отримання додаткового маржинального доходу від інтеграції у цифровий простір ЄС.

4. Виклад основного матеріалу.

Традиційні стратегії інформаційної безпеки (ІБ), розроблені для великих корпорацій, базуються на принципі «глибокої оборони» (defense in depth) та передбачають наявність значних капітальних інвестицій (CAPEX), виділеного штату

фахівців (CISO, SOC-аналітики) та статичної IT-інфраструктури. Однак для малих та середніх підприємств, особливо тих, що прагнуть інтеграції у Цифровий ринок ЄС, такий підхід виявляється неефективним з кількох причин:

1. Корпоративні рішення часто вимагають високих початкових витрат на ліцензування, апаратне забезпечення та розгортання. Для МСП, де бюджет на IT обмежений, такі витрати створюють критичне навантаження на грошові потоки (cash flow). Більше того, традиційні методи оцінки інвестицій (NPV, ROI) важко застосувати до ІБ у МСП, оскільки «прибуток» тут є непрямим – у вигляді уникнених збитків, які для малого бізнесу можуть бути фатальними (згідно зі статистикою, до 60% МСП закриваються протягом 6 місяців після серйозної кібер-атаки).

2. Стандартні рішення (наприклад, повномасштабні SIEM або SOAR системи) мають надлишкову функціональність, яка потребує постійного адміністрування. У МСП функцію ІБ часто виконує системний адміністратор-універсал або аутсорсингова компанія. Складність налаштування корпоративного ПЗ призводить до того, що значна частина функцій захисту залишається неактивною, що створює ілюзію безпеки при реальній вразливості.

3. МСП у процесі виходу на ринок ЄС проходять через стадії швидкого зростання або трансформації бізнес-моделей. Корпоративні системи захисту зазвичай інертні: вони важко піддаються швидкому масштабуванню «вниз» або «вгору» залежно від поточної кількості активів чи обсягів даних. Проєктно-орієнтований підхід, на противагу процесному, дозволяє розглядати безпеку як серію ітераційних покращень, що масштабуються разом із бізнесом.

4. Законодавчі акти ЄС вимагають від МСП не просто «наявності антивірусу», а доведеної стійкості (cyber resilience). Стандартні «коробкові» рішення часто не враховують специфіку галузевих вимог або транскордонних стандартів передачі даних. МСП потребують гнучких інструментів, які дозволяють швидко адаптувати протоколи безпеки під вимоги європейських партнерів без повної заміни інфраструктури.

Для українських МСП це означає, що безпека не може розглядатися лише як набір технічних заходів або «коробкових» рішень. Навпаки, вона має бути проєктно-орієнтованою, масштабованою і гнучкою**,** здатною швидко реагувати на зміни у бізнес-моделі та вимоги ринку. Ключовим завданням стає поєднання мінімізації фінансових і операційних ризиків із забезпеченням відповідності стандартам ЄС, які визначають, чи підприємство зможе брати участь у цифровому ринку та укладати контракти з європейськими партнерами.

Єдиний цифровий ринок Європейського Союзу (Digital Single Market) є складовою загальної стратегії інтеграції внутрішнього ринку ЄС і спрямований на забезпечення вільного руху даних, цифрових послуг, товарів та капіталу між державами-членами. Для українських МСП вихід на цифровий ринок ЄС означає не лише географічне розширення експорту, а й входження у високорегульоване правове середовище, де ключовим чинником доступу виступає дотримання вимог комплаєнсу у сфері захисту даних, кібербезпеки та цифрової відповідальності.

Систему регулювання цифрового ринку ЄС формує комплекс взаємопов’язаних нормативно-правових актів. Базовим документом у сфері захисту персональних даних є General Data Protection Regulation (GDPR, Регламент (ЄС) 2016/679) [8]. Він встановлює принципи законності обробки даних, мінімізації збору інформації, прозорості, підзвітності та обов’язковості повідомлення про витоки даних протягом 72 годин. Для МСП порушення вимог GDPR може призвести до штрафів у розмірі до 20 млн євро або до 4% глобального річного обороту. Водночас відповідність GDPR створює передумову для участі у транскордонних контрактах і цифрових ланцюгах постачання.

Другим ключовим актом є NIS2 Directive (Directive (EU) 2022/2555) [9], що регламентує заходи з підвищення загального рівня кібербезпеки в ЄС. NIS2 значно

розширює перелік суб'єктів, які підпадають під вимоги кіберстійкості, включаючи середні підприємства у критично важливих та цифрових секторах. Документ передбачає обов'язкове управління ризиками, впровадження політик безпеки, контроль ланцюгів постачання, регулярні аудити та персональну відповідальність керівництва за порушення.

Функціонування цифрових платформ регулюють також:

– Digital Services Act (DSA) [10] – встановлює правила відповідальності онлайн-платформ за контент, прозорість алгоритмів і захист прав користувачів;

– Digital Markets Act (DMA) [11] – спрямований на забезпечення чесної конкуренції на цифрових ринках, обмеження монопольних практик «gatekeepers»;

– Data Act [12]– регламентує доступ до промислових та IoT-даних і правила їх передачі між суб'єктами ринку.

Таким чином, для МСП вихід на цифровий ринок ЄС передбачає не лише формальне врахування окремих нормативно-правових актів, а й системну інтеграцію їхніх вимог у внутрішні бізнес-процеси, що фактично означає впровадження механізмів комплаєнсу. Комплаєнс у сучасному науковому розумінні трактується як системний управлінський процес забезпечення відповідності діяльності підприємства вимогам законодавства, галузевих стандартів, регуляторних актів та внутрішніх політик, інтегрований у структуру внутрішнього контролю та управління ризиками. Для малих і середніх підприємств комплаєнс означає інституціоналізацію процедур захисту даних, кібербезпеки, антикорупційної доброчесності та фінансової прозорості, що мінімізує регуляторні й репутаційні ризики та забезпечує доступ до цифрових ланцюгів постачання й транскордонних контрактів. У контексті виходу на ринок ЄС комплаєнс трансформується з витратної функції у стратегічний нематеріальний актив довіри, який підвищує конкурентоспроможність МСП і створює економічні передумови для стійкого розвитку. Для МСП комплаєнс включає:

– призначення відповідальної особи за захист даних (за потреби);
– проведення оцінки впливу на захист даних (DPIA);
– впровадження політик управління доступом і реагування на інциденти;
– документування процесів обробки інформації;
– регулярне навчання персоналу.

Але окрім нормативних актів і вимог комплаєнсу, українські МСП повинні орієнтуватися на об'єктивні показники цифрової готовності, які визначають їхню конкурентоспроможність на європейському ринку. Одним із ключових інструментів оцінки є Digital Economy and Society Index (DESI) [13], який вимірює рівень цифровізації економіки та суспільства в країнах ЄС. За останніми даними, лише близько 55% малих і середніх підприємств у ЄС мають базовий рівень цифрової інтенсивності [14], тобто достатній для ефективного використання цифрових платформ, електронної комерції та онлайн-сервісів. Для українських МСП, що прагнуть інтеграції у цифровий ринок ЄС, досягнення цього рівня є обов'язковою умовою конкурентоспроможності. Недостатня цифрова інтенсивність обмежує можливості укладати транскордонні контракти, брати участь у тендерах, а також зменшує привабливість компанії для європейських інвесторів і партнерів.

Водночас сучасний регуляторний ландшафт ЄС значно ускладнює доступ до цифрового ринку для підприємств із недостатньо розвиненою інформаційною безпекою. Нова Директива NIS2 (Directive (EU) 2022/2555) [9] розширює сферу застосування вимог кіберстійкості, включаючи середні підприємства з чисельністю від 50 працівників, що раніше могли не підпадати під обов'язкові норми. Директива передбачає управління ризиками, впровадження політик безпеки, регулярні аудити та персональну відповідальність керівництва за порушення. Таким чином, NIS2 створює прямий юридичний стимул для інвестування в інформаційну безпеку та формує нову

мінімальну планку комплаєнсу для МСП, без досягнення якої доступ до цифрового ринку ЄС стає обмеженим або неможливим.

Поєднання цифрової готовності за DESI та вимог кіберстійкості за NIS2 підкреслює, що для українських МСП комплаєнс та інформаційна безпека є не просто технічними або юридичними зобов'язаннями, а стратегічними елементами конкурентоспроможності. Впровадження ефективних систем управління ризиками, навчання персоналу та інтеграція процедур комплаєнсу дозволяють підприємствам не лише уникати штрафів і санкцій, а й отримувати прямі економічні вигоди: можливість укладати контракти, забезпечувати безперервність бізнесу та будувати репутаційний капітал на висококонкурентному європейському ринку. Саме тому доцільно перейти від абстрактних міркувань про «необхідність захисту» до кількісної оцінки потенційних втрат і економічного ефекту від їх мінімізації.

Традиційний підхід до оцінки інвестицій в IT-інфраструктуру часто не враховує специфіку ризиків кібербезпеки. Для МСП, що інтегруються у цифровий ринок ЄС, ключовим показником доцільності інвестиційного проєкту є коефіцієнт рентабельності інвестицій у безпеку – ROSI (Return on Security Investment).

Тому першим кроком у математичному обґрунтуванні є визначення показника очікуваних річних збитків (ALE – Annual Loss Expectancy) до впровадження проєкту:

$$ALE = SLE \times ARO, \tag{1}$$

де *SLE (Single Loss Expectancy)* – очікуваний збиток від одного інциденту (вартість втрачених даних, простою обладнання, штрафів за порушення GDPR тощо);

ARO (Annual Rate of Occurrence) – ймовірність виникнення інциденту протягом року (статистичний показник для конкретної галузі чи регіону).

З урахуванням проєктно-орієнтованого підходу, рентабельність конкретного проєкту з інформаційної безпеки (*ROSIproj*) розраховується за формулою:

$$ROSI = \frac{(ALE \times P) - Cost_{proj}}{Cost_{proj}}, \tag{2}$$

де *P (Mitigation Ratio)* – коефіцієнт ефективності захисного рішення (яку частку ризику нівелює даний проєкт, зазвичай 0 < P < 1);

Costproj – сукупна вартість впровадження та підтримки проєкту.

Дані таблиці 1 демонструють, як разові інвестиції в інформаційну безпеку (ІБ) корелюють із ризиками та фінансовими показниками підприємства в розрізі трьох років (типовий період планування для МСП).

Аналіз *ALE* свідчить, що навіть якщо штраф у €20 000 здається малоймовірним, математичне очікування збитків у €2 000 щороку створює постійний тиск на бюджет МСП. У той же час від'ємне значення ROSI у перший рік є типовим для проєктно-орієнтованого підходу, оскільки основні витрати (€5 000) припадають на початковий етап. Проте вже на третій рік сукупні «заощаджені» збитки (€2 000 × 3 роки × 0,95 = €5 700) перевищують вартість інвестиції, що підтверджує стратегічну доцільність проєкту. Тому для МСП важливо розуміти, що інвестиція у €5 000 фактично «страхує» актив вартістю €20 000, що є критичним для збереження платоспроможності підприємства при виході на цифрові ринки ЄС.

Таблиця 1. Розрахунок економічної ефективності інвестиційного проєкту з ІБ для МСП (гіпотетичний сценарій)

Показник	Символ	Значення	Пояснення значення
Очікуваний збиток від одного інциденту (штраф GDPR)	SLE	€20 000	Потенційна сума фінансових санкцій за порушення
Ймовірність виникнення інциденту протягом року	ARO	10% (0,1)	Статистична частота успішних атак на МСП у галузі
Річні очікувані збитки (без системи захисту)	ALE	€2 000	Середньорічний фінансовий ризик (€20 000 × 0,1)
Вартість інвестиційного проєкту з ІБ	Cost	€5 000	Витрати на впровадження та ліцензування (CAPEX)
Коефіцієнт зниження ризику після впровадження	P	95% (0,95)	Ефективність рішення у запобіганні інцидентам
Показник ROSI (за перший рік)	ROSI	-62%	Короткостроковий показник (інвестиція ще не окупилася)
Показник ROSI (сумарно за 3 роки)	ROSI	+14%	Проєкт виходить на прибутковість за рахунок уникнення збитків

Джерело: складено автором на основі власних розрахунків.

Для підприємств, що інтегруються до Цифрового єдиного ринку ЄС, інвестиції в ІБ слід розглядати не лише через призму уникнення збитків (ROSI), а й як створення стратегічного активу – вартості доступу до ринку (*Market Access Value, MAV*). У сучасних умовах європейські контрагенти висувають жорсткі вимоги до кіберстійкості партнерів (ланцюгів постачання). Таким чином, за відсутності підтвердженого рівня ІБ, підприємство стикається з «нульовим доступом», де потенційний дохід від експорту дорівнює нулю.

Тому ми пропонуємо застосовувати модифікована модель чистої вигоди (Net Benefit):

$$NB = (ALE \times P) + \Delta MAV - Cost_{proj}, \quad (3)$$

де *(ALE×P)* – фінансова вигода від зниження ризиків (запобігання штрафам та простоям);

ΔMAV – прогнозований приріст маржинального доходу, отриманий завдяки виконанню вимог комплаєнсу ЄС (можливість укладати контракти з партнерами з ЄС);

Costproj – інвестиційні витрати на проєкт.

Для проєктно-орієнтованого управління доцільно використовувати матрицю, що класифікує інвестиції за їх впливом на ринкові можливості (таблиця 2).

Таблиця 2. Класифікація інвестицій відповідно до їх впливу на рівень ризику та можливість доступу МСП до відповідного ринку

Тип інвестиційного проєкту	Вплив на ризик (ALE)	Вплив на ринок (MAV)	Пріоритет для МСП
Критичний комплаєнс (наприклад, GDPR)	Високий	Критичний (дозвіл на роботу)	1
Технічний захист (наприклад, Firewall)	Високий	Низький (технічна вимога)	2
Сертифікація (наприклад, ISO 27001)	Середній	Високий (конкурентна перевага)	3

Джерело: складено автором на основі власних розрахунків.

Отже, включення *ΔMAV* у розрахунки дозволяє змінити фінансову картину проєкту:

1) без врахування *MAV* проєкт може мати тривалий термін окупності (2 – 3 роки);

2) із врахуванням *MAV* (додаткових контрактів, які стали можливими після сертифікації) інвестиція часто стає рентабельною вже у перші 6 – 12 місяців.

Модифікована модель чистої вигоди (NB) показує, що фінансовий ефект від проєкту формується не лише за рахунок запобігання ризикам (ALE×P), а й завдяки додатковим ринковим можливостям (ΔMAV), які відкриваються після виконання вимог комплаєнсу чи сертифікації.

Для оцінки чутливості запропонованої моделі чистої вигоди до зміни параметра ΔMAV доцільно застосувати сценарний підхід. За базових припущень (SLE = €20 000, ARO = 0,1; відповідно ALE = €2 000 на рік; коефіцієнт зниження ризику P = 0,95; вартість проєкту Costproj = €5 000; горизонт оцінки – 3 роки) річна вигода від мінімізації ризиків становить €1 900, або €5 700 за три роки (табл. 3). Подальший фінансовий результат залежить від приросту вартості доступу до ринку (ΔMAV), що формується завдяки виконанню вимог комплаєнсу.

Таблиця 3. Сценарний аналіз ефективності модифікованої моделі NB (3 роки)

Показник	Консервативний	Помірний	Оптимістичний
ΔMAV (за 3 роки), €	3 000	9 000	18 000
Запобігання збиткам (ALE×P×3), €	5 700	5 700	5 700
Сукупна вигода, €	8 700	14 700	23 700
Costproj,	5 000	5 000	5 000
NB (3 роки), €	+3 700	+9 700	+18 700
Орієнтовний строк окупності	2,2 роки	1,1 року	< 1 року

Джерело: складено автором на основі власних розрахунків.

Результати розрахунків свідчать, що навіть за консервативного сценарію інвестиція залишається фінансово доцільною, тоді як у помірному та оптимістичному варіантах ефект ΔMAV суттєво прискорює окупність проєкту. Це підтверджує, що врахування приросту ринкових можливостей у структурі моделі NB трансформує інвестиції в інформаційну безпеку з інструменту мінімізації ризиків у стратегічний фактор формування доданої вартості та конкурентоспроможності МСП на цифровому ринку ЄС.

Отримані результати узгоджуються з міжнародною статистикою, яка демонструє високий фінансовий масштаб кіберризиків для МСП. Згідно зі звітом IBM «Cost of a Data Breach» [15], середня вартість витоку даних для організацій із менш ніж 500 працівниками у 2025 році становила приблизно €3 – 3,2 млн., що для малого бізнесу може означати катастрофічні фінансові наслідки. Водночас більшість МСП витрачає на кібербезпеку менше 5% свого IT-бюджету, тоді як експертні рекомендації радять виділяти 10 – 15% для досягнення адекватної кіберстійкості [16].

Поєднання запропонованих підходів дозволяє зробити висновок: інвестиції у проєктно-орієнтовану безпеку повинні враховувати не лише прямий захист від інцидентів, а й потенціал відкриття нових ринкових можливостей, що часто робить такі проєкти економічно виправданими навіть для МСП із обмеженими ресурсами. Таким чином, розрахунок NB із ΔMAV допомагає аргументовано планувати бюджет на кібербезпеку та цифрову трансформацію, зменшуючи ризики втрат і підвищуючи рентабельність інвестицій.

5. Висновки та перспективи подальших досліджень в даному напрямку.

У результаті проведеного дослідження доведено, що в умовах інтеграції до Єдиного цифрового ринку ЄС інформаційна безпека малих та середніх підприємств має розглядатися не як сукупність неминучих витрат, а як стратегічна інвестиційна складова, що забезпечує ринкову стійкість та конкурентоспроможність. Обґрунтовано, що перехід до проєктно-орієнтованого управління дозволяє МСП ефективно розподіляти обмежені фінансові ресурси, впроваджуючи заходи захисту ітераційно та адаптуючи їх до динамічних вимог європейського законодавства.

Встановлено, що ключовим фактором економічної доцільності таких інвестицій є не лише мінімізація потенційних збитків від кіберінцидентів, оцінених через показник ALE, а й отримання додаткової вартості від доступу до високомаржинальних цифрових ринків Євросоюзу. Запропонована модель оцінки чистої вигоди, що включає показник приросту вартості доступу до ринку (ΔMAV), демонструє, що виконання вимог регламенту GDPR та директиви NIS2 виступає обов'язковою умовою подолання нетарифних бар'єрів у цифровій транскордонній торгівлі.

Математичне моделювання за показником ROSI підтвердило, що проєкти з інформаційної безпеки для МСП мають високу рентабельність, оскільки запобігання репутаційним та фінансовим втратам у поєднанні з розширенням клієнтської бази в ЄС забезпечує окупність інвестицій у середньостроковій перспективі. Таким чином, синергія проєктного підходу та інвестиційного аналізу створює дієвий механізм для трансформації системи управління інформаційною безпекою вітчизняних підприємств відповідно до стандартів цифрової економіки.

Подальший розвиток цього напряму досліджень доцільно зосереджувати на розробці автоматизованих систем підтримки прийняття рішень для динамічного перегляду портфеля проєктів з безпеки залежно від зміни ландшафту кіберзагроз та оновлення регуляторної бази ЄС.

Author details (in English)

THE INVESTMENT COMPONENT OF PROJECT-ORIENTED INFORMATION SECURITY MANAGEMENT FOR SMALL AND MEDIUM ENTERPRISES ON THE PATH TO THE EU DIGITAL MARKET

Olena SOROKIVSKA | **Nazar KINAL** | **Ruslan STEFANIV**

Ternopil Ivan Puluj National Technical University
56 Ruska str., Ternopil, 46001, Ukraine

e-mail: sorokivska_o@tntu.edu.ua
ORCID ID: https://orcid.org/0000-0001-8549-2910

e-mail: nazarkinal@ukr.net
ORCID ID: https://orcid.org/0009-0003-7980-2101

e-mail: amrg-pg@ukr.net
ORCID ID: https://orcid.org/0009-0002-2129-3454

Abstract. *The article examines the investment dimension of project-oriented information security management in small and medium-sized enterprises (SMEs) within the context of integration into the European Union's digital market. It substantiates that the entry of Ukrainian SMEs into the EU Digital Single Market is accompanied by a dual challenge: the need for accelerated digital transformation of business processes and the simultaneous alignment of risk management systems with the requirements of the European regulatory framework. It is argued that information security is no longer a supporting IT function but has evolved into a strategic determinant of competitiveness and market access. The study analyzes the impact of key EU regulatory acts – particularly the General Data Protection Regulation (GDPR) and the NIS2 Directive – on shaping cybersecurity and resilience requirements for enterprises engaged in cross-border activities. It is demonstrated that compliance in the areas of personal data protection and cybersecurity functions not only as a regulatory obligation but also as an economic prerequisite for participation in digital supply chains, access to investment, and the conclusion of contracts with European partners. The methodological framework combines instruments of investment management with a project-based approach to information security governance. The study proposes the application of the Annual Loss*

Expectancy (ALE) indicator and the Return on Security Investment (ROSI) metric to provide a quantitative justification for cybersecurity investments under conditions of limited financial resources typical for SMEs. Furthermore, a modified Net Benefit (NB) model is developed by incorporating the concept of Market Access Value (ΔMAV). This extended model captures not only the financial effect of risk mitigation and avoided penalties but also the additional marginal revenue generated through compliance-driven access to the EU market. Based on a hypothetical financial scenario, the analysis demonstrates that even when ROSI is negative in the short term, investments in information security become economically justified in the medium term. When ΔMAV is incorporated into the assessment, such projects may generate positive financial returns within the first years of implementation. The paper also substantiates that a low level of information security creates regulatory, financial, reputational, and supply-chain barriers that significantly hinder the entry of Ukrainian SMEs into the EU digital market. In conclusion, the transformation of information security management from a cost-based perception to an investment-oriented model is identified as a necessary condition for ensuring business resilience, competitiveness, and successful integration of Ukrainian SMEs into the European digital economic space. The proposed methodological approach can serve as a practical analytical tool for strategic cybersecurity budgeting and investment decision-making in the process of European economic integration.

Keywords: *investment management, information security, SMEs, project-oriented management, digital transformation, EU market, ROSI.*

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at http://sepd.tntu.edu.ua/images/stories/pdf/2026/26soaedm.pdf

Funding

The authors received no direct funding for this research.

Citation information

Sorokivska, O., Kinal, N. & Stefaniv, R. (2026) The investment component of project-oriented information security management for small and medium enterprises on the path to the EU digital market. Socio-Economic Problems and the State (electronic journal), Vol. 34, no. 1, pp. 71-82. URL: http://sepd.tntu.edu.ua/images/stories/pdf/2026/26soaedm.pdf

Використана література:

1. Markowitz H. M. Portfolio Selection. *The Journal of Finance*. 1952. Vol. 7, No. 1. P. 77–91. DOI: https://doi.org/10.1111/j.1540-6261.1952.tb01525.x
2. Sharpe W. F. Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. *The Journal of Finance*. 1964. Vol. 19, No. 3. P. 425–442. DOI: https://doi.org/10.2307/2977928
3. Kerzner H. *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*. 13th ed. Hoboken, NJ : John Wiley & Sons, 2022.
4. Humphrey W. S. *Managing Technical People: Innovation, Teamwork, and the Software Process*. Reading, MA : Addison-Wesley, 1997.
5. Verizon. *2025 Data Breach Investigations Report*. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 18.01.2026).
6. *ZipDo Education Reports 2026. Small Business Cyber Security Statistics*. URL: https://zipdo.co/ (дата звернення: 20.01.2026).
7. ENISA. *Cybersecurity Threat Landscape for SMEs*. URL: https://www.enisa.europa.eu/ (дата звернення: 22.01.2026).
8. Угода між Україною та Європейським Союзом про участь України у програмі «Цифрова Європа». URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 24.01.2026).

9. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 24.02.2026).
10. Digital Services Act. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act (дата звернення: 30.01.2026).
11. Digital Markets Act. URL: https://digital-markets-act.ec.europa.eu/index_en (дата звернення: 10.02.2026).
12. Data Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (дата звернення: 10.02.2026).
13. Digital Economy and Society Index (DESI). URL: https://digital-strategy.ec.europa.eu/en/policies/desi (дата звернення: 12.02.2026).
14. Strutynsk I., Kozbur H., Melnyk L., Dmytrotsa L., Sorokivska O. Bridging the Digital Divide: A Tailored Digital Maturity Model for SME Transformation // Ermolayev V. et al. (eds.). *Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2025*. Communications in Computer and Information Science. Vol. 2763. Cham : Springer, 2025. DOI: https://doi.org/10.1007/978-3-032-10477-9_16.
15. How Much Will a Data Breach Cost in 2025? | *Cybersecurity Insights*. URL: https://www.sangfor.com/blog/cybersecurity/data-breach-cost-2025 (дата звернення: 14.02.2026).
16. Cybersecurity Statistics For Small Businesses 2025. URL: https://www.totalassure.com/blog/cyber-attacks-on-small-businesses-statistics-2025 (дата звернення: 14.02.2026).

References

1. Markowitz H. M. Portfolio Selection. The Journal of Finance. 1952. Vol. 7, No. 1. P. 77–91. DOI: https://doi.org/10.1111/j.1540-6261.1952.tb01525.x
2. Sharpe W. F. Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk. The Journal of Finance. 1964. Vol. 19, No. 3. P. 425–442. DOI: https://doi.org/10.2307/2977928
3. Kerzner H. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. 13th ed. Hoboken, NJ : John Wiley & Sons, 2022.
4. Humphrey W. S. Managing Technical People: Innovation, Teamwork, and the Software Process. Reading, MA : Addison-Wesley, 1997.
5. Verizon. 2025 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (accessed: 18.01.2026).
6. ZipDo Education Reports 2026. Small Business Cyber Security Statistics. URL: https://zipdo.co/ (accessed: 20.01.2026).
7. ENISA. Cybersecurity Threat Landscape for SMEs. URL: https://www.enisa.europa.eu/ (accessed: 22.01.2026).
8. Uhoda mizh Ukrainoiu ta Yevropeiskym Soiuzom pro uchast Ukrainy u prohrami «Tsyfrova Yevropa» [Agreement between Ukraine and the European Union on Ukraine's participation in the Digital Europe Programme]. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (accessed: 24.01.2026).
9. Dyrektyva Yevropeiskoho Parlamentu i Rady (IeS) 2022/2555 vid 14 hrudnia 2022 roku [Directive of the European Parliament and of the Council (EU) 2022/2555 of 14 December 2022]. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (accessed: 24.02.2026).
10. Digital Services Act. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act (accessed: 30.01.2026).

11. Digital Markets Act. URL: https://digital-markets-act.ec.europa.eu/index_en (accessed: 10.02.2026).
12. Data Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-act (accessed: 10.02.2026).
13. Digital Economy and Society Index (DESI). URL: https://digital-strategy.ec.europa.eu/en/policies/desi (accessed: 12.02.2026).
14. Strutynska I., Kozbur H., Melnyk L., Dmytrotsa L., Sorokivska O. Bridging the Digital Divide: A Tailored Digital Maturity Model for SME Transformation // Ermolayev V. et al. (eds.). Information and Communication Technologies in Education, Research, and Industrial Applications. ICTERI 2025. *Communications in Computer and Information Science*. Vol. 2763. Cham : Springer, 2025. DOI: https://doi.org/10.1007/978-3-032-10477-9_16.
15. How Much Will a Data Breach Cost in 2025? | Cybersecurity Insights. URL: https://www.sangfor.com/blog/cybersecurity/data-breach-cost-2025 (accessed: 14.02.2026).
16. Cybersecurity Statistics For Small Businesses 2025. URL: https://www.totalassure.com/blog/cyber-attacks-on-small-businesses-statistics-2025 (accessed: 14.02.2026).

Socio-Economic Problems and the State (ISSN: 2223-3822) is published by Academy of Social Management (ASM) and Ternopil Ivan Puluj National Technical University (TNTU), Ukraine, Europe.
Publishing with SEPS ensures:
• Immediate, universal access to your article on publication
• High visibility and discoverability via the SEPS website
• Rapid publication
• Guaranteed legacy preservation of your article
• Discounts and waivers for authors in developing regions
Submit your manuscript to a SEPS journal at http://sepd.tntu.edu.ua